(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :14/02/2024

(21) Application No.202411010324 A
(43) Publication Date : 23/02/2024

(54) Title of the invention : SYSTEM AND METHOD FOR ENDPOINT DETECTION WITH DYNAMIC ATTACK PROCESS TREE NAVIGATION

(51) International classification :G06N0020000000, G06F0021550000, H04L0009000000, G06F0021570000, G06F0021560000
(86) International Application No :NA
Filing Date :NA
(87) International Publication No : NA
(61) Patent of Addition to Application Number :NA
Filing Date :NA
(62) Divisional to Application Number :NA
Filing Date :NA

(71)**Name of Applicant :**
1)Chitkara University
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ---------- ----------
2)Bluest Mettle Solutions Private Limited
Name of Applicant : NA
Address of Applicant : NA
(72)**Name of Inventor :**
1)MISHRA, Rahul
Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India. Pune ---------- ----------
2)SINGH, Dhiraj
Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India. Pune ---------- ----------
3)GARG, Dhruv
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ---------- ----------

(57) Abstract :
An endpoint detection and response (EDR) system (102) with dynamic attack process tree is disclosed. The system (102) autonomously detects and identifies threats within endpoint devices (104) and network environments (106), employing real-time analysis of attack process trees to identify cyber attack patterns. A unique feature is the incorporation of a threat correlation engine, which correlates information from various sources, facilitating comprehensive threat analysis. The disclosed EDR system adapts to evolving cyber threats by utilizing machine learning to dynamically evaluate issue severity and activate tailored responses. Furthermore, the system (102) contributes to building resilient digital infrastructures in alignment with sustainable development goal 16. This system (102) combines threat detection, analysis, and adaptive response strategies for enhanced cybersecurity.

No. of Pages : 25 No. of Claims : 9